NOVEL METHODS FOR ENABLING PUBLIC KEY SCHEMES IN FUTURE MOBILE SYSTEMS

N. Komninos, B. Honary

Lancaster University (UK)

ABSTRACT

It is essential to enable public key schemes in future mobile systems to solve current problems in authentication and key management for end-to-end security. In this paper, we propose new procedures for enabling public key schemes in future mobile terminals. The proposed procedures are based on the complex public key computations that can be performed either in the SIM card or in the terminal itself. Multiple crypto-processors are also used to decrease the processing time required to perform the complex public key computations.

INTRODUCTION

The security mechanisms of current mobile systems (i.e. GSM) are implemented in three different system elements; the subscriber identification module (SIM), the mobile station (MS), and the mobile network. The SIM contains the international mobile subscriber identity (IMSI), the individual subscriber authentication key (Ki), the ciphering key generating algorithm (A8), the authentication algorithm (A3), as well as a personal identification number (PIN). The MS contains the ciphering algorithm (A5). The algorithms A3, A5, and A8 are also present in the GSM network. The authentication centre (AUC) consists of a database of identification and authentication information for subscribers. This information consists of the IMSI, the temporarily MSI (TMSI), the location area identity (LAI), and the Ki for each user [1). In order for the authentication and security mechanisms to function, all three elements (SIM, MS, network) are required as shown in Figure 1.

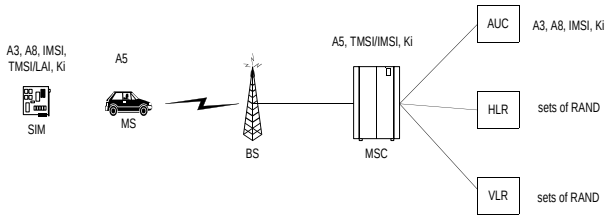


Figure 1 -- Secure Structure of GSM Network

Moreover, MS are activated by the SIM card. By inserting the card into any mobile telephone and entering the correct PIN password, MS is registered to network and all calls are charged to the SIM card owner. Such a SIM card has a micro central processing unit (CPU), a random access memory (RAM), a read only memory (ROM), and an electrically erasable programmable read only memory (EEPROM) chip.

The memory available in the SIM cards and general in integrated circuits, such as smart cards, brings enormous flexibility to the storage allocation as shown in Table 1. There are a number of smart cards available on the market today that provide security services for electronic commerce purposes. Public key generation, digital signatures, and key distribution protocols have already been implemented by some vendors such as Certicom (SC-500 model with RSA/DSA/ECC key generation, RSA/DSA/ECDSA signature, RSA/DH/ECDH key agreement) (4).

Memory	Typical	Maximum
ROM	8 – 16 kBytes	32 kBytes
EEPROM	2 – 8 kBytes	16 kBytes
RAM	128 – 256 Bytes	512 – 1000 Bytes

Table 1 – Memory Sizes

Nowadays, RSA signatures and verifications are supported with a choice of 512, 768, or 1024 bit key lengths. The algorithms typically use the Chinese Remainder Theorem (CRT) in order to speed up the processing. Even at the 1024 bit key length, the time needed to perform a signature is typically under one second. Usually the EEPROM file that contains the private key is designed such that the sensitive key material never leaves the chip. Even the cardholder can't access the key material in this case. The usage of the private key is protected by the user's PIN, so that possession of the card does not imply the ability to sign with the card. RSA's public key cryptography standards (PKCS#1) padding is implemented in some cards. The Digital Signature Algorithm (DSA) is less widely implemented than RSA. When it is implemented, it is typically found only at the 512 bit key length.

Even though smart cards have the ability to generate public key pairs, this can be very slow. Typical times needed for a 1024 bit RSA key pair ranges from 8 seconds to 3 minutes. The larger times violate the ISO specifications for communications timeout so

specialized hardware, such as co-processors, is sometimes necessary. The lack of computing power implies a relatively weak random number source as well as relatively weak algorithms for selecting large prime numbers, which results in bad quality of the key pairs.

SECURE INFRASTRUCTURE

Public key schemes can be enabled in future mobile systems with the memory available in SIM cards. The secure infrastructure of a future mobile network using public key schemes is shown in Figure 2. The public key algorithm (PKA), such as RSA, can be either a software implementation in the SIM card or a hardware implementation in the mobile itself. Furthermore, the PKA should also be located either in the mobile switching centre (MSC) or in the authentication centre (AUC) for the subscriber's authentication and key distribution process.

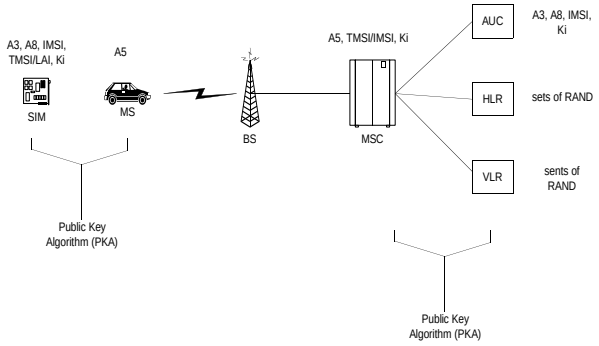


Figure 2 – Public Key Schemes in Future Mobile Systems

However, public and secret key schemes involve several "expensive" computations such as factoring a number, finding the discrete logarithm of a number, and performing modular exponentiation over finite fields. An additional cryptographic module is required to perform these complex computations for the combined public and secret key schemes. Addition, subtraction, multiplication, modular division, exponentiation, and logarithmic functions can be computed in a crypto-processor. Several secure infrastructures can be proposed depending on where the crypto-processor is located. It can be located in the **SIM card** and/or in the **mobile terminal** itself.

When it is located in the SIM card there are two proposed schemes. In the first scheme, the cryptographic algorithms, public key pairs, and certificates can be generated offline by the manufacture, and uploaded to the ROM chip in a SIM card (Figure 3). Current implementations of public key algorithms in smart cards have shown that the storage allocation required by the algorithms is 800 bytes (3). A total of 4 Kbytes is required when key pairs and multiple certificates are included.

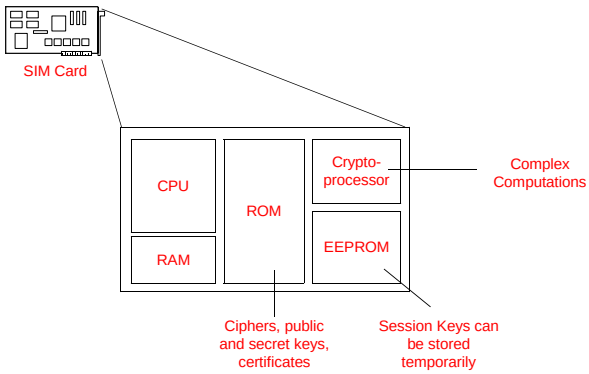


Figure 3 – Secure Infrastructure using SIM Card

In this scheme, some complex computations have been reduced since public key pairs, and certificates have been generated offline. Authentication is a one-step process; certificates can be used to authenticate users and networks. Multiple certificates apply to multiple networks. Furthermore, a session key can be generated by the subscriber and stored temporary in EEPROM. The subscriber who initiates a call can type some random numbers from the keypad to generate a random session key just before a call is established. Finally, in the session key distribution phase public key encryption and decryption is performed in the crypto-processor.

In the second scheme, generation of public key pairs and certificates can take place in the mobile terminal itself. In this scheme two or more crypto processors can be used in parallel to increase the overall processing power and reduce the real time generation of keys, certificates, and public key encryption/decryption. Authentication, key distribution and session key generation can follow the same principle like in the first scheme. When the crypto-processor is located in the mobile terminal, there are two approaches.

In the first approach, a second SIM card with an embedded crypto-processor is used for complex computations. The cryptographic algorithms, message digests, and the card's operating system are stored in ROM. Cipher keys and random numbers are stored in EEPROM. Therefore, authentication and session key generation can follow the same principle like in scheme one.

In the second approach the crypto-processor is located in the baseband of the mobile terminal. Then public key complex computations can be calculated in parallel from two crypto-processors based on their mathematical complexity. The cryptographic algorithms, message digests, keys and random numbers are stored in the SIM like the first case. Finally, authentication and session key generation can follow the same principle as in scheme one.

IMPLEMENTATION / RESULTS

Public key algorithms are divided in two procedures; public key generation and public key encryption/decryption. In order for the end user to generate the public key pair, prime number generation must take place. Generation of prime numbers is a three-step process; generate a random number P, then check if P is not divisible by any small primes: 3, 5, 7, 11 etc, and finally apply CRT. Steps two and three can be performed simultaneously in two different crypto-processors. Moreover, the final public key pair usually results from modular exponentiations calculations $(m^e \bmod n)$.

Similarly, in the public key encryption and decryption process modular exponentiation calculations are mainly required. Therefore, modular $(m \bmod n)$ and exponentiation calculation (m^e) can be performed simultaneously.

When two or more crypto processors are used, parallel processing of public key computations can be enabled using the Application Protocol Data Unit (APDU) protocol specified in ISO 7816-4. The APDU protocol is an application-level protocol used by the mobile terminal to send commands (C-APDU) in half-duplex mode to the SIM cards and vice-versa (R-APDU) (2). The C-APDU is followed by the R-APDU as illustrated in Figure 4a and 4b.

CLA	INS	P1	P2	P3	DATA

CLA: Class Instruction; 'A0' is used in GSM
INS: Instruction Command
P1, P2, P3: Instruction Parameters
DATA: Data Field

(a) C-APDU

DATA	SW1	SW2

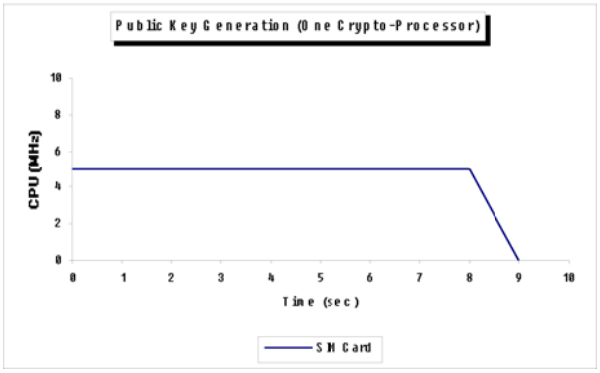
DATA: Data Field
SW1: Status Words

(b) R-APDU

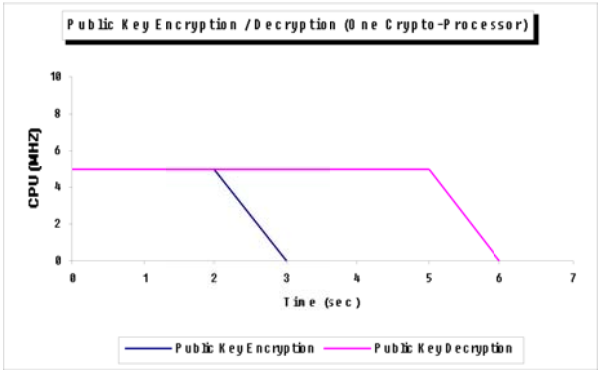
Figure 4 – (a) Command APDU, (b) Response APDU

Instruction commands can be used to declare the mathematical computation to be processed. Moreover, instruction parameters can be used to assign priorities based on the complexity of the computations. Complex computations such as modular exponentiation can be processed in the crypto-processor located in the mobile terminal. Once the bits in the data field have been processed accordingly the results can be sent back (R-APDU) and used by the encryption algorithms in the SIM card.

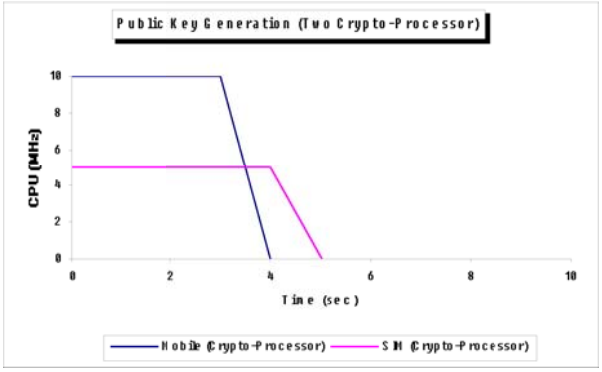
Nowadays, the CPU of a SIM card comprises an 8 bit controller in 5MHz and is in most instances a variant of a 6805 processor (e.g. Motorola, SGS-Thomson), a 8051 processor (i.e. Philips, Siemens) or a manufacturer specific CPU. Furthermore, the CPU of a mobile terminal comprises a 12-16 bit controller in 10MHz and again varies accordingly. The results shown in Figure 5 were obtained using Crypto-flex smart cards (3) from Schlumberger. Crypto-flex smart cards have special math co-processors to perform complex computations. The RSA public key pair used was 1024-bit.



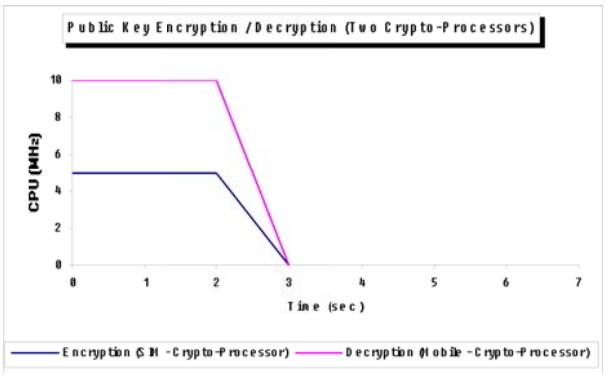
(a)



(b)



(c)



(d)

Figure 6 – (a) Public key generation when crypto - processor is located in the SIM Card
(b) Public Key encryption/decryption when crypto-processor is located in the SIM Card
(c) Public key generation two crypto-processors are used
(d) Public Key encryption/decryption when two crypto-processors are used

When one crypto-processor is used, which is located in the SIM card, public key generation needs about 9 seconds (Figure 6a). On the other hand, when two crypto-processors are used, which are located in the SIM card and in the mobile terminal, public key generation requires 5 seconds only (Figure 6c). Similarly, public key encryption and decryption needs 6 and 3 seconds with one or two crypto-processors respectively (Figure 6b, 6d).

CONCLUSION

It is essential to enable public key schemes in future mobile systems to solve current problems in authentication and key management for end-to-end security. Several secure infrastructures were proposed which require additional hardware based on the location of the crypto-processors. When only one crypto-processor is used, located in the SIM card, public key pair generation needs about 9 seconds. On the other hand, when two crypto-processors are used, one in the SIM card and the other in the mobile terminal, public key pair generation requires 5 seconds only. Similarly, public key encryption and decryption needs 6 and 3 seconds with one or two crypto-processors respectively.

Multiple crypto-processors are necessary to reduce the time needed to perform public key computations. There are trade-offs, such as expenses and power consumption, between the number and the processing power of crypto-processors. The price of the SIM card and therefore, of a mobile phone increases dramatically when a crypto-processor is used. Furthermore, the power consumption of the crypto-processors with high processing power decreases the battery life. However, two crypto-processors from 10 to 30 MHz are required to enable public key schemes and drop the real time encryption/decryption to 1 second. Then, authentication and key distribution can take place in an acceptable time.

ACKNOWLEDGEMENTS

Special thanks to HW Communications Limited for their financial support.

REFERENCES

(1) M. Mouly, M. Pauter, "The GSM System for Mobile Communications", GSM Forum, 1992

(2) ETSI, "Specifications of the Subscribers Identity Module – Mobile Equipment (SIM-ME) interface (GSM 11.11)", July 1996

(3) Schlumberger Cryptoflex Smart Cards http://www.cryptoflex.com/

(4) Soon-Yong Choi, Andrew B. Whinston, "White Paper – Smart Cards Enabling Smart Commerce in the Digital Age", KPMG and Centre for Research in Electronic Commerce, The University of Texas at Austin, 1998